Legal Issues Regarding Digital Forensic Examiners Third Party Consent to Search

Thomas Lonardo
Gabelli College of Business
Roger Williams University
One Old Ferry Road
Bristol, RI 02809
401-254-3580
tlonardo@rwu.edu

Tricia P. Martland
School of Justice Studies
Roger Williams University
One Old Ferry Road
Bristol, RI 02809
401-254-3353
tmartland@rwu.edu

Doug White
Center for Forensics, Applied Networking and Security
School of Justice Studies
Roger Williams University
One Old Ferry Road
Bristol, RI 02809
401-254-3165
dwhite@rwu.edu

Alan Rea
Haworth College of Business
Western Michigan University
1903 West Michigan Avenue
Kalamazoo, MI 49008-5412
269-387-4247
rea@wmich.edu

ABSTRACT

This paper focuses on Federal law as it relates to consent to search relating to Fourth Amendment privacy in the practice of Digital Forensics. In particular, Digital Examiners should be aware of how decisions in Federal Court may impact their ability to acquire evidence in both civil and criminal settings. Digital Forensics, being a relatively new field, is particularly subject to change as cases and appeals are decided. This paper provides an overview of relevant case law relating to issues in Digital Forensics. More importantly, our research provides Digital Forensic Examiners (DFE), as defined by Lonardo, White, and Rea (2008, 2009), with scenarios that illustrate the various nuances when dealing with the consent to search. From issues of common authority, conflicting consent, apparent authority, and voluntary consent, our research explores court findings and applies them to practical advice and policy formation for DFEs.

Keywords: digital forensics, case study, consent to search, federal law, fourth amendment

1. INTRODUCTION

In this paper, we address current developments in the law relating to third party "consent to search" and the Fourth Amendment within the practice of Digital Forensics as defined by Lonardo, White, and Rea (2008). The various issues relating to third party consent are illustrated through various federal circuit court cases and the US Supreme Court and represent the challenges and issues of which one needs to be aware. This is critical as the legal environment surrounding Digital Forensics is rapidly developing as judges and attorneys undertake a more informed technical and legal analysis. For the Digital Forensic Examiner (DFE) these cases will provide insights to DFEs how the courts view computer forensics by way of evidentiary, fourth amendment and other legal issues raised on appeal.

We have organized this paper by the primary facets of comment authority, conflicting consent, apparent authority, and voluntary consent. Each major topical area is discussed with supporting relevant case law to illustrate how the courts approach each relevant DFE issue. Please note that given the limited precedent regarding the subject matter, courts often rely on analogies that are not computer technology based and we do the same. However, we do place it within a DFE context. Before proceeding, we need to provide not only our definition of Digital Forensic Examiners but also situate it within the context of the Fourth Amendment.

1.1 Defining Digital Forensic Examiners

The role of Digital Forensic Examiners has increased within legal casework in the last ten years. As a result, the scope of the profession, increased salaries, and number of examiners has grown immensely due to the need in most evidentiary circumstances for expertise in digital media examination (White, Micheletti, & Glorfeld, 2008; White, Michelletti, Glorfeld, & Rea, 2006). This increased involvement in all facets of law and government has led to challenges for DFEs, states, and the courts in determining the nature and definition of the DFE role.

These challenges require us to examine just what defines a Digital Forensic Examiner (DFE). Many researchers have approached the definition, but we will follow the definition put forth by Lonardo et al. (2008) because it is used as a framework on which state statutes and other accrediting bodies have been analyzed:

> A Digital Examiner deals with extracting, gathering, and analyzing data from a computer or computers, networks, and other digital media with subsequent preparation of reports and opinions of this media for evidentiary or other states purposes such as data/digital security, audit, or assessment. [See also Lonardo et al. (2009)].

Although this definition seems straightforward, as the DFE role's purview has

expanded into more and more courtrooms, the questions of the breadth of the examiner in terms of procurement of evidence have also increased not only in terms of the processes in place but also the technology examined. Our focus in this paper is the technology because advances have produced situations requiring greater and greater levels of expertise in the procurement of both civil and criminal evidence and, as a result, created a need to review the relevant court opinions on these issues.

1.2 The Fourth Amendment of the Constitution of the United States

Digital Forensic Examiners, who are not practicing as officers of the court or in other law enforcement roles, are not subject to the Fourth Amendment. However, the continued push for "privacy" and "information privacy" has led many examiners to include custodial approvals and other "permissions" in their civil collection procedures. In this light, the idea of the Fourth Amendment is pervasive in the practice of digital forensics and is a focus of our paper.

In summary, the Fourth Amendment pertains to *government activity* in searches, not those by private parties unless the private party is deemed as an agent for the government (i.e. law enforcement.):

> The right of the people to be secure in their persons, houses, papers, and effects, against ***unreasonable searches and seizures***, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized. (***Emphasis added***)

The concept of third party consent to search revolves around the Fourth Amendment of the United States Constitution and specifically is concerned as to whether the person has a reasonable expectation of privacy in the location that is searched ("Katz v. U.S.," 1967). However, the Fourth Amendment does not specifically speak of a "reasonable expectation of privacy" because it is a doctrine of law set forth by the US Supreme Court (USSC) in cases interpreting whether a search is "unreasonable."

Practice demonstrates that the higher the expectation of privacy, the higher the protected rights are from searches, and the higher the likelihood a search warrant would be required. The courts analyze the "totality of the circumstances" for each case under review ("Illinois v. Rodriguez," 1990). This means that a particular court reviews the facts on a case-by-case basis in making a determination whether third party consent is valid. As a result, there is no "bright line rule" as to what makes a search based on third party consent legal and valid, thereby making this a challenge. However, the crux of the question can hinge on situations where consent given to law enforcement is found to be knowing and voluntary, thereby

not implicating the Fourth Amendment and making the search and/or seizure valid ("Schneckloth v. Bustamonte," 1973).

As a result of the voluntary delineation, one of the most critical focuses in digital forensics is the idea of "consent." Consent is most dramatically at the forefront when examiners are involved in a situation where a family member or other third party "gives permission" to examine another person's media or device. In civil examinations, it is common for IT administrators, HR representatives, or other members of the corporate management team to grant a Digital Forensic Examiner the permission to review or obtain evidence from digital media. In these cases the computer and its contents are typically the property of the company or business and the employee has no possessory or legal rights.

However, outside of the corporate content, many questions regarding the nature of consent and the right to examine both media and data becomes an issue for the DFE. In the following sections we examine cases that detail situations in which the express permission of the actual owner of that evidence may not be apparent and can hamper the DFE's ability to review and produce usable evidence.

2. COMMON AUTHORITY

The concept of common authority directly relates to the idea that multiple parties may have access to, or some level of control over, media that is not necessarily shared but may be accessed communally. For example, portable media such as a USB flash drive that is plugged into a roommate's computer.

Digital Forensics Issue: If the roommate consents to the examination of his personal computer, does this consent include the roommate's USB flash drive plugged into the computer?

Common authority might be simply defined as "When a party has free access and the authority to enter an area or use an item, that item/area is under common authority." The U.S. Supreme Court underscores this definition:

> The authority which justified the third-party consent does not rest upon the law of property, with its attendant historical and legal refinement, but rests rather on mutual use of the property by persons generally ***having joint access or control for most purposes***, so that it is reasonable to recognize that any of the co-inhabitants has the right to permit the inspection in his own right and that the others have assumed the risk that one of their number might permit the common area to be searched. ("Georgia v. Randolph," 2006) [quoting ("United States v. Matlock," 1974)] (***Emphasis added***)

2.1 Conflicting Consent and Computer Drives

However, a critical issue that emerges from this definition is conflicting consent. Consider the Georgia v. Randolph ("Georgia v. Randolph," 2006) case:

Facts: Estranged wife gave police consent to search the home. She previously moved in with some relatives for a few weeks and it was not clear whether she was moving back permanently to reconcile or was there to pick up personal effects. Both the estranged wife and husband were physically present. The husband denied consent and the wife granted the consent to search. Police entered the home and searched it finding traces of drugs and ultimately obtaining a warrant.

Issue: When a co-tenant objects to a search of an apartment or home in the presence of the consenting co-tenant does that objection override the consenting party where both have common authority over the premises?

Court's ruling: First, the ability to grant consent rests with whether the person granting the consent has "common authority" to do so. In other words, does the consenting party have free access and authority to certain areas of the home or apartment shared by both habitants? Secondly, even if one person has the common authority, if the cohabitant with shared common authority and access is physically present and refuses to grant the authority then law enforcement must abide by the non-consenting cohabitant's wishes.

Digital Forensic Implications: Thus, Randolph might imply that a spouse/partner might be able to grant consent particularly when an item is shared or an area of the drive is shared between multiple parties. It would not be the case that this would grant consent to search protected or privileged areas of the drive or device belonging to a spouse/partner.

However, Randolph would not perhaps cover the aforementioned USB flash drive as illustrated in the following case ("United States v. King," 2010) in which a non-consenting party's ownership of the hard drive installed in consenting party's computer was granted by the third party.

Facts: Person who resided with the defendant was arrested and consented to a seizure of the personal computer (PC) that she owned. King assisted with the surrender by disconnecting the PC. King told police he installed the hard drive on the PC and claimed ownership of it. He then asked law enforcement if he could remove it as the owner. Police refused his request. In searching the PC certain incriminating email correspondence was found between the owner of the PC and King. This correspondence led to a search warrant of the defendant's home and the seized computer. As a result of this search the police found thousands of images of child pornography in addition to the incriminating emails. King voluntarily met with police and after several hours admitted having sexual

relations with the daughter of the PC owner. Ultimately, King pled guilty for having engaged in a sexual act with a person under the age of 12 according to 18 U.S.C. (UnitedStates, 2010a). Later, King attempted to withdraw his plea, but a lower court denied his request.

Issue: At issue here is "when an owner of a computer consents to its seizure, does that consent include the computer's hard drive even when it was installed by another who claims ownership of it and objects to its seizure?" ("United States v. King," 2010).

Court's ruling: The defendant looked to Georgia v. Randolph ("Georgia v. Randolph," 2006) as a basis to negate the consent of the PC owner. The Lower court relied on United States v. Matlock ("United States v. Matlock," 1974) in its decision to uphold the guilty plea and sentencing. The Lower court reasoned that both parties had common authority over the PC and its hard drive. The Superior court found neither case controlling and stated "the facts of this case place it somewhere between those cases" ("United States v. King," 2010).

The Superior court found that the rule in Randolph ("Georgia v. Randolph," 2006) does not go beyond the consent to search a home and does not apply to the personal effects within. In this sense, the court follows Andrus' comparison of a computer to a container and notes, "A computer is a personal effect" ("United States v. Andrus," 2007) [cited in ("United States v. King," 2010)]. In this approach the court used the "common authority" rule in Matlock ("United States v. Matlock," 1974) in which both parties had access to the PC, shared passwords, email accounts etc. Therefore, there was no reasonable expectation of privacy and each party had the authority to grant consent regardless of whether one may had refused the consent, unlike Randolph ("Georgia v. Randolph," 2006).

Digital Forensic Implications: Returning to our original scenario of Roommate A plugging in a USB flash drive into Roommate B's laptop. Roommate B gives consent to examine the laptop. Does this consent extend to the flash drive?

This would appear to be a similar case to King ("United States v. King," 2010). In King, the officers did not permit the owner to remove a hard drive attached to a computer, but the drive was permanently installed inside the case. In this practical scenario the issue for digital forensic examiners would be whether the acquisition of peripherals connected and in a multi-party residence extends to multiple roommates sharing one computer/laptop. Thus, this scenario is similar to the case of King ("United States v. King," 2010), and DFEs should be able to seize all the peripherals attached to a common machine because consent has been granted by one of the parties who accesses to the machine.

3. APPARENT AUTHORITY

Moving from the idea of common authority and the communal access to media, we now examine the concept of apparent authority and the perception that someone has the authority within a particular scenario. In other words, when someone has the reasonable belief that they have appropriate authority to conduct an examination of certain media based on circumstances presented to him or her, they should be permitted to do so. For instance, if a law enforcement officer is given consent to examine the media, the officer may assume that person has the right to give this consent if the surrounding circumstances presented to the officer would lead him/her to reasonably believe that person has the authority to do so, even if they are not the actual owner or custodian of the computer or in fact do not have actual authority. United States v. Andrus (2007) illustrates factors that must be taken into consideration when making this determination.

Digital Forensic Issue: A partner surrenders a cell phone and indicates that the phone may be examined. Subsequently, the partner provides the pin login code for the phone to the examiners.

3.1 Password Protected Files

Facts: Defendant pled guilty to one count of possession of child pornography, in violation of 18 U.S.C. 2252(a) (4) (B) (UnitedStates, 2010b). However, he retained the right to appeal the denial of his suppression motion by the district court during an investigation of a third-party billing and credit card company that provided subscribers with access to websites containing child pornography. The investigation of the company, Regpay, led the Agents of the Bureau of Immigration and Customs Enforcement (ICE) to investigate the subscribers, one of them being the defendant, Ray Andrus.

Records reflected three people lived at the residence in question, two of which were the defendant and his 91-year-old father, Dr. Andrus. The agent and the police officer, with a verbal and signed consent, as well as the assistance of Dr. Andrus, searched the room of Ray Andrus and analyzed his PC with EnCase forensic software (GuidanceSoftware, 2010). This investigation led to the direct access of the hard drive. There was no need to determine if the hard drive required any user name or password. During this search certain .jpg files where found to contain child pornography on the hard drive.

The search was temporarily suspended when law enforcement discovered this was the only PC in the house and that Dr. Andrus was not the likely user. Thus, actual authority may not have existed. However, the defendant subsequently gave consent when law enforcement confronted him with their discovery. After bringing the PC back to law enforcement headquarters it was later discovered there was a user profile (with individual user name and password) for Ray

Andrus.

Issue: This is a case of "first impression" meaning that this is the first time third party consent relating to a computer has been addressed by the 10th Circuit Court of Appeals. The issue before the court was whether there was apparent authority to consent to the search by the defendant's father. The court needed to consider the following information discovered by law enforcement personnel via an interview with the third party, Dr. Andrus:

- Dr. Andrus owned the house and lived there with family members.
- Dr. Andrus' house had Internet access. Dr. Andrus paid the Internet and cable bill.
- The email address associated with Dr. Andrus' account had been activated and used to register on a website that provided access to child pornography.
- Ray Andrus lived in the center bedroom. Law enforcement also knew that Dr. Andrus had access to the room at will. This implied that Dr. Andrus had access to the computer.

Court's ruling: The court in this case stated that where there is either actual or apparent authority to consent by a third party based on the totality of the circumstances, the consent by the third party would be valid. The court described ***actual authority*** as follows:

> A third party has actual authority to consent to a search "if that third party has either (1) mutual use of the property by virtue of joint access, or (2) control for most purposes" ("United States v. Andrus," 2007) [See also Matlock where holding "common authority over or other sufficient relationship to the premises or effects sought to be inspected" may give rise to a third party's valid consent to search ("United States v. Matlock," 1974).]

Where actual authority may be lacking ***apparent authority*** will suffice as stated by the court:

> Whether apparent authority exists is an objective, totality-of-the-circumstances inquiry into whether the facts available to the officers at the time they commenced the search would lead a reasonable officer to believe the third party had authority to consent to the search. ("Illinois v. Rodriguez," 1990) ["[W]here an officer is presented with ambiguous facts related to authority, he or she has a duty to investigate further before relying on the consent." ("United States v. Kimoana," 2004).]

Given the above findings, we must consider the following factors when examining third party consent and how it applies within apparent authority in the examination of digital media. If law enforcement has knowledge or reasonably suspects that files are password protected, then the third party consent would not be valid. Password protection implies a high degree of expectation of privacy. However if law enforcement sees no perceived protection relating to computer access the court states that "under our case law, however, officers are not obligated to ask questions unless the circumstances are ambiguous ("United States v. Kimoana," 2004). In short, if law enforcement *reasonably believes* apparent authority exists, they have no affirmative duty to inquire further regarding password-protected files. The court rejected the dissent's opinion asserting that it is typical for computers to have password protection. Since there was no data or facts on the record to substantiate this, the court did not go further into this inquiry.

Therefore, we would argue that if the physical location of the computer is such that a reasonable person would believe other members of the household had common access to the computer, including the third party, the consent might be valid. However if the third party disclaims access to the computer or files even if the computer is in a common area, third party consent might not be valid. ("Trulock v. Freeh," 2001)

Digital Forensic Implication: In our practical example of one partner turning over his/her partner's cell phone and the pin code number the examiner of the phone could reasonably assume that the person has the authority to consent to a search of the phone. However, if the examiner had doubts (viz. the name on the phone or other information), he/she would be obligated to further investigate before assuming that there was authority to consent.

4. THIRD PARTY OWNERSHIP INTEREST IN PREMISES AND COMMON AUTHORITY

Conflating common authority and potential apparent authority, we must consider the scenario with multiple partners in residence who might jointly use a particular piece of technology. This idea is typical with one party being the "owner" and the other party residing in the residence. A common example would be a computer in a dorm room owned by one roommate but used by others in the same area. In this section we examine a case ("United States v. Nichols," 2009) that illustrates factors that must be considered when making this determination.

Digital Forensics Issue: Can the examiner seize a laptop found in an apartment with consent from a third party who does not own the property, but is at the residence?

Facts: Defendant Nichols lived with his girlfriend and her seven year old daughter in a house owned solely by defendant. Girlfriend had lived in the home for past three months, paying bills and receiving mail at the home. Moreover, she had unrestricted access to the house and property in the house, including defendant's computer. The girlfriend found an unlabeled computer disc with sexually explicit photos of her daughter and gave the disc to the police. Based on the contents of the disc, the police obtained a search warrant for Nichols' computer and found matching sexually explicit photos as were on the computer disc.

Issue: Defendant challenged the district court's denial of his motion to suppress evidence obtained during the search of his home and computer. He claimed the search was not authorized by a warrant. Defendant also asserted that his girlfriend, who lived in Nichols' home but did not own the property, did not have the authority to consent to a search of Nichols' home and computer.

Court's Ruling: The court cited Matlock which states that a "warrantless search is valid where the consent to search is from a third party who possesses common authority over the premises or effects" ("United States v. Matlock," 1974). Common authority is described as a question of fact determined by factors such as mutual use, joint access, and control ("United States v. Almeida Perez," 2008).

In this case, the girlfriend was a co-occupant of the home, enjoying unrestricted access to the house and the computer. The court found that the girlfriend occupied the house as a possessor, giving the girlfriend the authority to consent to the search of the home and the computer.

In addition to common authority, the Court stated the girlfriend had "apparent authority." Such authority is present when the "facts available to the officer at the moment…warrant a man of reasonable caution in the belief that the consenting party had authority over the premises" ("United States v. Almeida Perez," 2008). In this situation the defendant's girlfriend met the police at the door of the home, appeared familiar with the house, and freely operated the computer. These facts suggest that the defendant's girlfriend is an occupant of the house capable of granting consent.

The court did not address Nichol's claim that the police did not have a warrant, but included in the facts portion of the opinion that police had obtained a warrant prior to searching the home.

Digital Forensics Implication: In our laptop example, if the person granting access was a resident of the apartment, even if they were not necessarily the owner/rent payer, they would have the common authority to grant access to the laptop under this case as well as the other cases cited in this paper, particularly apparent authority.

5. VOLUNTARY CONSENT

In this section we revisit the issue of passwords and the associated privacy expectations in the context of the Fourth Amendment and its application within a technological framework. Most illustrative of a potential scenario is the high-profile case of the United States v. Trulock ("United States v. Notra Trulock, Linda Conrad," 2001).

Digital Forensics Issue: One of the more common challenges hinges on the ability of one party to give the password for another party in a case. This happens often in an organizational situation when one person provides the password for another employee's desktop.

5.1 Search of Password Protected Files

Facts: Notra Trulock served as Director of Intelligence for the Department of Energy (DOE) and later as the Director of the Office of Counter Intelligence. Trulock alleged that he found evidence of a serious security breach at the Los Alamos weapons Nuclear Laboratory by Chinese spies. He further alleged that the CIA ignored his repeated warnings about the breach.

The breach was eventually made known to Congress and Trulock testified at congressional hearings. Sometime later Trulock was demoted at DOE and ultimately forced out in 1999. He documented the security breach and the "blind eye" of the CIA in a manuscript later published in the National Review (Trulock, 2000a). Trulock contended that the government retaliated because of his published account of the issues.

Trulock lived in a townhouse along with property owner Linda Conrad, a co-complainant. Conrad was Executive Assistant to Trulock during his tenure at DOE. She then reported to Trulock's successor Lawrence Sanchez. On July 14, 2000 Conrad alleged that Sanchez told her the FBI wanted to question her about Trulock and informed her that FBI agents had a warrant to search the townhouse. Moreover she claimed that Sanchez told her the agents would "break down the front door in the presence of the media if she refused to cooperate" (Trulock, 2000b).

Two FBI agents arrived at the DOE and escorted Conrad to a conference room. Agents were armed but did not display their weapons. During the three-hour interview there were no allegations of raised voices or threats, but at some point Conrad wished to make or answer phone calls. The record is unclear whether or not agents told her she could or could not make the calls.

During the interview agents questioned Conrad about Trulock's personal records and computer files. Conrad told agents she shared a computer with him, but each maintained separate password protected files on the hard drive. Conrad noted that they did not know each other's passwords and could not access each other's files.

Agents gave Conrad a consent form and asked her to sign. There was no mention of a search warrant or threat to "break down the door." Conrad alleged she was both crying and shaking. At the townhouse, Trulock asked to see the search warrant and agents told him Conrad had signed consent paperwork to search. Agents searched the computer files for 90 minutes, including Trulock's password protected files. The agents took custody of the hard drive before leaving the townhouse.

Issues: A number of claims were presented by plaintiffs, including two important questions:

1. Was Conrad's consent involuntary?
2. Was Conrad's consent, if voluntary, sufficient to permit the search of Trulock's private computer files?

Court's Ruling: Two major issues the court considered focused on voluntary consent first of the warrant and second of the computer search of password protected files. Under ("Schneckloth v. Bustamonte," 1973), valid consent is recognized as an exception to the Fourth Amendment prohibition against warrantless searches. However, consent to search is valid only if the consent was knowing and voluntary under the "totality of the circumstances" test ("United States v. Mendenhall," 1980).

In this case, the court found Conrad's consent to be invalid under the "Bumper" rationale, which states, "the acquiescence to an assertion of lawful authority does not constitute an understanding, intentional and voluntary waiver of rights under the 4th amendment…where there is coercion there cannot be consent" ("Bumper v. North Carolina," 1968).

Agents conducting the townhouse search never claimed to have a warrant; however, Sanchez told Conrad the FBI possessed a warrant. The court found Sanchez conveyed this message at the behest of the FBI and was acting in concert with the FBI. Based on these facts, Conrad's consent was found to be involuntary. (Despite this finding by the Court, the agents were found to have qualified immunity.)

In terms of the computer search, plaintiffs contended that the search of Trulock's password protected computer files violated the Fourth Amendment. The court, already having found Conrad's consent to be involuntary, determined that even if consent had been voluntary, Conrad was not authorized to consent to a search of Trulock's password protected files.

In its findings, the court stated that valid third party consent must pass a two-prong test. First, the third party must have the authority to consent and second, the consent must be voluntary. Authority to consent is found by "mutual use of the property by persons generally having joint access or control for most purposes, so that it is reasonable to recognize that any of the co-inhabitants has the right to

permit the inspection in his own right and that others have assumed the risk that one of their number might permit the common area to be searched" ("United States v. Matlock," 1974).

Ultimately, the court found Conrad lacked the authority to properly consent to a search of Trulock's password protected files. Despite mutual use of the computer kept in Conrad's bedroom, both Conrad and Trulock kept their files separate, as well as protected by passwords and neither of them disclosed their passwords to each other. While the court recognized that Conrad had the authority to consent to a general search of the computer, her authority "did not extend to Trulock's password protected files" ("Trulock v. Freeh," 2001).

To make this determination the court relied on the Block case ("United States v. Block," 1978). In this case, the Block court held that the defendant's mother had authority to consent to a search of defendant's room in the home they shared, but the authority did not extend to a "locked footlocker located within the room. The authority to consent cannot be thought automatically to extend to the interiors of every discrete enclosed space capable of search within the area…the rule has to be one of reason that assesses the critical circumstances indicating the presence or absence of a discrete expectation of privacy with respect to the particular object" ("United States v. Block," 1978).

In its decision, the court considered Trulock's password protected files to be analogous to Block's locked footlocker. By using a password, Trulock affirmatively intended to exclude Conrad and others from his personal files. Thus, Trulock had a reasonable expectation of privacy for the password-protected files and Conrad's authority did not extend to them. (Despite this finding, the Court again found qualified immunity for the actions of the agents in the improper search.)

Digital Forensics Implications: Thus, it would appear that if another party provides the password, it would be a violation on any files/areas protected by that password so long as the items weren't shared. If the items were shared (even with different logins) it would seem that the search could proceed.

6. OVERALL POLICY IMPLICATIONS

We would be remiss not to stress the need for Digital Forensic Examiners (DFE) and law enforcement to communicate frequently with one another to promote knowledge exchange. It is one of the most effective means to bridge procedural gaps between the two areas as they increasingly work in conjunction with each other in diverse cases. This is especially important because as more DFEs enter the profession from non-law enforcement backgrounds, we will experience an increase in privacy violations that will lead to evidence challenges in court.

Ultimately, it is imperative for Digital Forensic Examiners (DFE) to set policies in

order to ensure privacy in each individual case to minimize the impact of privacy violations. We recommend that several key policies areas must be implemented:

1. The recovery of password-protected files should only be conducted with the express consent of the owner of the file (the person who created the password).
2. Seizure of peripherals should be acceptable even if the peripheral belongs to a third party as long as it is attached to the seized device.
3. Third parties should be able to provide consent for devices that are located in common areas.
4. Third parties should be able to provide consent for files that are in shared media space.

While we realize that these rules apply specifically to law enforcement, it prudent to implement these guidelines to receive consent in the same context in civil investigations to avoid later challenges to collected evidence.

7. CONCLUSION

In this paper we have provided several United States Federal courts' key cases that can provide direction to the DFE practitioner. In our research we argue that DFEs should be aware of how decisions in various Federal Courts may impact their ability to acquire evidence in both civil and criminal settings. Digital Forensics, being a relatively new field, is particularly subject to changing and evolving law as cases and appeals are decided. We have found that as the field develops, judges and attorneys are undertaking a more informed technical and legal analysis.

While these cases apply to law enforcement, it is prudent for practicing DFE professionals to be aware of challenges that may emerge against procured digital evidence. This is particularly applicable to private investigators practicing Digital Forensics who will frequently encounter diverse types of consent situations.

Ultimately, our research provides critical insight to Digital Examiners on how the courts view computer forensics by way of evidentiary, fourth amendment and other legal issues brought on appeal. Given the limited precedent regarding the subject matter, courts often rely on analogies that are not computer technology based. Through our research, we were able to apply an analysis of these cases into the technical realm.

AUTHOR BIOGRAPHIES

Tom Lonardo is an Assistant Professor of Security Assurance Law and Business Law at Roger Williams University in Bristol, RI. Tom is an attorney and a member of the Rhode Island and Massachusetts Bar. Tom's research focuses on legal issues relating to Security and Digital Forensics.

Tricia Martland is an Assistant Professor of Legal Studies at Roger Williams University. Tricia's research interests focus on criminal legal issues, particularly digital forensics, domestic violence and juvenile law. Tricia is an attorney and a member of the Rhode Island Bar Association and a former Special Assistant Attorney General for the state of Rhode Island.

Doug White is a Professor of Forensics, Networking, and Security at Roger Williams University in Bristol, RI. Doug is also a member of the Rhode Island Cyber Disruption Team and works as an independent consulting in forensics and security. Doug teaches Digital Forensics and Computer Networking courses. Doug primarily conducts research in Security and Digital Forensics.

Alan Rea is a Professor of Computer Information Systems at the Haworth College of Business, Western Michigan University in Kalamazoo, MI. At WMU, Alan teaches courses in programming, information security management, and Web and mobile application security. Alan's current research involves a combination of artificial intelligence, security, social engineering, and virtual reality.

REFERENCES

Bumper v. North Carolina, 391 (U. S. 543 1968).

Charles Katz v. United States, 389 U.S. 347, 88 S.Ct. 507 (19 L.Ed.2d 576 1967).

Georgia v. Randolph, 547 U.S. 103, 126 S.Ct. 1515 (164 L.Ed.2d 208 2006).

Guidance Software. (2010). EnCase.

Illinois v. Rodriguez (497 U.S. 177, 181 1990).

Lonardo, T., White, D., & Rea, A. (2008). To license or not to license: An examination of state statutes regarding private investigators and digital examiners. *The Journal of Digital Forensics, Security, and Law, 3*(3), 1-13.

Lonardo, T., White, D., & Rea, A. (2009). To license or not to license revisited: An examination of state statutes regarding private investigators and digital examiners. *The Journal of Digital Forensics, Security, and Law, 4*(3), 1-16.

Schneckloth v. Bustamonte (412 U.S. 218 1973).

Trulock, N. (2000a). FBI Hits Back at Trulock. *National Review* Retrieved July 6, 2011, from http://old.nationalreview.com/comment/comment071700c.html

Trulock, N. (2000b). Excerpts from the NR article that led to the FBI seizure of the author's computer. Retrieved July 6, 2011, from http://old.nationalreview.com/comment/comment071700d.html

Trulock v. Freeh, F.3d 391, 403 (4th Cir. 2001).

United States v. Almeida Perez, 549 F.3d 1162 (8th Cir. 2008).

United States v. Andrus, 483 F.3d 711 (10th Cir. 2007).

United States v. Block, 590 F.2d 535, 539 (4th Cir. 1978).

United States v. Kimoana, 383 F.3d 1215 (10th Circuit 2004).

United States v. King, 09-1861 (Third Circuit 2010).

United States v. Matlock, 415 U.S. 164, 94 S.Ct. 988 (39 L.Ed.2d 242 1974).

United States v. Mendenhall, 446 (U.S. 557 1980).

United States v. Nichols, 574 F. 3d 633, 636 (8th Cir. 2009).

United States v. Notra Trulock, Linda Conrad, 275 F. 3d 391 (4th Cir. 2001).

White, D., Micheletti, C., & Glorfeld, L. (2008). A Longitudinal Analysis of Trends in Digital Forensics Professionals. *Decision Sciences International Conference*, Baltimore, MD, November, 2008.

White, D., Michelletti, C., Glorfeld, L., & Rea, A. (2006). Who Are the CyberSleuths?: A Demographic Analysis of Computer Forensics Professionals. *Decision Sciences International Conference*, San Antonio, TX, November 18-21, 2006.

18 U.S.C. Aggravated Sexual Abuse, 2241 C.F.R. (2010a).

18 U.S.C. Certain activities relating to material involving the sexual exploitation of minors, 2252(a)(4)(B) C.F.R. (2010b).